

Amendments to the Claims

1 Claim 1 (currently amended): A computer program product for enabling an identity change
2 during a certificate-based host access session, said computer program product embodied on a
3 computer-readable medium and comprising:

4 computer-readable program code means for processing a first sign-on during a secure
5 session using a digital certificate, further comprising:

6 computer-readable program code means for establishing said secure session from a
7 client machine to a server machine using said digital certificate, wherein said digital certificate
8 represents an identity of said client machine or a user thereof;

9 computer-readable program code means for storing said digital certificate or a
10 reference thereto at said server machine;

11 computer-readable program code means for establishing a session from said server
12 machine to a host system using a legacy host communication protocol, responsive to receiving, at
13 said server machine, a first sign-on request from said client machine, wherein said first sign-on
14 request identifies a first secure legacy host application to which said first sign-on is requested;

15 computer-readable program code means for passing said stored digital certificate
16 or said reference from said server machine to a host access security system;

17 computer-readable program code means, operable in said host access security
18 system, for authenticating said identity using said passed digital certificate or a retrieved
19 certificate which is retrieved using said reference;

20 computer-readable program code means, operable in said host access security
21 system, for using said passed or retrieved digital certificate to locate access credentials for said

Serial No. 09/619,912

-2-

Docket RSW9-2000-0081-US1

22 user;

23 computer-readable program code means, operable in said host access security
24 system, for accessing a stored password or generating a password substitute representing said
25 located credentials;

26 computer-readable program code means, operable in said host access security
27 system, for returning said stored password or generated password substitute to said server
28 machine, along with a first user identifier corresponding to said located credentials;

29 computer-readable program code means for requesting by said first secure legacy
30 host application, responsive to said computer-readable program code means for establishing said
31 session, first sign-on information for said user, and

32 computer-readable program code means for responding to said request for first
33 sign-on information by sending a first sign-on message with placeholder syntax from said client
34 machine to said server machine, said placeholder syntax representing a user identification and a
35 password of said user, wherein said user identification and said password are expected in said first
36 sign-on message by said first secure legacy host application; and

37 computer-readable program code means, operable in said server machine, for using
38 said returned password or password substitute and said returned first user identifier to
39 transparently complete said first sign-on, on behalf of said user of said client machine, to said first
40 secure legacy host application executing at said host system by substituting said returned first user
41 identifier and said returned password or password substitute for said placeholder syntax in said
42 first sign-on message, thereby creating a revised first sign-on message, and forwarding said
43 revised first sign-on message from said server machine to said first secure legacy host application;

44 and

45 computer-readable program code means for processing a second sign-on during said
46 secure session, without requiring establishment of a new secure session between said client
47 machine and said server machine, using a second digital certificate that represents a second
48 identity, further comprising:

49 computer-readable program code means for receiving a second sign-on request, at
50 said server machine from said client machine, wherein: (1) said second sign-on request identifies
51 a second secure legacy host application to which said second sign-on is requested; (2) said second
52 sign-on request includes said second digital certificate, or a second certificate reference that
53 references said second digital certificate, for said second identity; (3) said second secure legacy
54 host application may be identical to said first secure legacy host application; and (4) said second
55 identity is for a second user, wherein said second user may be identical to said user;

56 computer-readable program code means for passing said second digital certificate
57 or said second certificate reference from said server machine to said host access security system;

58 computer-readable program code means, operable in said host access security
59 system, for authenticating said second identity using said passed second digital certificate or a
60 second retrieved certificate which is retrieved using said second certificate reference;

61 computer-readable program code means, operable in said host access security
62 system, for using said passed second digital certificate or said second retrieved certificate to
63 locate second access credentials for said second user,

64 computer-readable program code means, operable in said host access security
65 system, for accessing a second stored password or generating a second password substitute

66 representing said second located credentials;
67 computer-readable program code means, operable in said host access security
68 system, for returning said second stored password or second generated password substitute to
69 said server machine, along with a second user identifier corresponding to said second located
70 credentials; and
71 computer-readable program code means, operable in said server machine, for using
72 said returned second password or second password substitute and said returned second user
73 identifier to transparently complete said second sign-on, on behalf of said second user of said
74 client machine, to said second secure legacy host application executing at said host system.

1 Claim 2 (previously presented): The computer program product as claimed in Claim 1, wherein
2 said digital certificate and said second digital certificate are X.509 certificates and said digital
3 certificate reference and second certificate reference are references to an X.509 certificate.

1 Claim 3 (original): The computer program product as claimed in Claim 1, wherein said
2 communication protocol is a 3270 emulation protocol.

1 Claim 4 (original): The computer program product as claimed in Claim 1, wherein said
2 communication protocol is a 5250 emulation protocol.

1 Claim 5 (original): The computer program product as claimed in Claim 1, wherein said
2 communication protocol is a Virtual Terminal protocol.

Serial No. 09/619,912

-5-

Docket RSW9-2000-0081-US1

1 Claim 6 (original): The computer program product as claimed in Claim 3, wherein said host
2 access security system is a Resource Access Control Facility (RACF) system.

1 Claim 7 (previously presented): The computer program product as claimed in Claim 1, wherein
2 said computer-readable program code means for processing said second sign-on further comprises
3 computer-readable program code means for storing said second digital certificate at said server
4 machine.

Claim 8 (canceled)

1 Claim 9 (currently amended): A system for enabling an identity change during a certificate-based
2 host access session, comprising:

3 means for processing a first sign-on during a secure session using a digital certificate,
4 further comprising:

5 means for establishing said secure session from a client machine to a server
6 machine using said digital certificate, wherein said digital certificate represents an identity of said
7 client machine or a user thereof;

8 means for storing said digital certificate or a reference thereto at said server
9 machine;

10 means for establishing a session from said server machine to a host system using a
11 legacy host communication protocol, responsive to receiving, at said server machine, a first sign-

Serial No. 09/619,912

-6-

Docket RSW9-2000-0081-US1

on request from said client machine, wherein said first sign-on request identifies a first secure legacy host application to which said first sign-on is requested;

means for passing said stored digital certificate or said reference from said server machine to a host access security system;

means, operable in said host access security system, for authenticating said identity using said passed digital certificate or a retrieved certificate which is retrieved using said reference;

means, operable in said host access security system, for using said passed or retrieved digital certificate to locate access credentials for said user;

means, operable in said host access security system, for accessing a stored password or generating a password substitute representing said located credentials;

means, operable in said host access security system, for returning said stored password or generated password substitute to said server machine, along with a first user identifier corresponding to said located credentials;

means for requesting by said first secure legacy host application, responsive to said computer-readable program code means for establishing said session, first sign-on information for said user; and

means for responding to said request for first sign-on information by sending a first sign-on message with placeholder syntax from said client machine to said server machine, said placeholder syntax representing a user identification and a password of said user, wherein said user identification and said password are expected in said first sign-on message by said first secure legacy host application; and

34 means, operable in said server machine, for using said returned password or
35 password substitute and said returned first user identifier to transparently complete said first sign-
36 on, on behalf of said user of said client machine, to said first secure legacy host application
37 executing at said host system by substituting said returned first user identifier and said returned
38 password or password substitute for said placeholder syntax in said first sign-on message, thereby
39 creating a revised first sign-on message, and forwarding said revised first sign-on message from
40 said server machine to said first secure legacy host application;; and

41 means for processing a second sign-on during said secure session, without requiring
42 establishment of a new secure session between said client machine and said server machine, using
43 a second digital certificate that represents a second identity, further comprising:

44 means for receiving a second sign-on request, at said server machine from said
45 client machine, wherein: (1) said second sign-on request identifies a second secure legacy host
46 application to which said second sign-on is requested; (2) said second sign-on request includes
47 said second digital certificate, or a second certificate reference that references said second digital
48 certificate, for said second identity; (3) said second secure legacy host application may be identical
49 to said first secure legacy host application; and (4) said second identity is for a second user,
50 wherein said second user may be identical to said user;

51 means for passing said second digital certificate or said second certificate reference
52 from said server machine to said host access security system;

53 means, operable in said host access security system, for authenticating said second
54 identity using said passed second digital certificate or a second retrieved certificate which is
55 retrieved using said second certificate reference;

56 means, operable in said host access security system, for using said passed second
57 digital certificate or said second retrieved certificate to locate second access credentials for said
58 second user;

59 means, operable in said host access security system, for accessing a second stored
60 password or generating a second password substitute representing said second located
61 credentials;

62 means, operable in said host access security system, for returning said second
63 stored password or second generated password substitute to said server machine, along with a
64 second user identifier corresponding to said second located credentials; and

65 means, operable in said server machine, for using said returned second password
66 or second password substitute and said returned second user identifier to transparently complete
67 said second sign-on, on behalf of said second user of said client machine, to said second secure
68 legacy host application executing at said host system.

1 Claim 10 (previously presented): The system as claimed in Claim 9, wherein said digital
2 certificate and said second digital certificate are X.509 certificates and said digital certificate
3 reference and second certificate reference are references to an X.509 certificate.

1 Claim 11 (original): The system as claimed in Claim 9, wherein said communication protocol is a
2 3270 emulation protocol.

1 Claim 12 (original): The system as claimed in Claim 11, wherein said host access security system

2 is a Resource Access Control Facility (RACF) system.

1 Claim 13 (previously presented): The system as claimed in Claim 9, wherein said means for
2 processing said second sign-on further comprises means for storing said second digital certificate
3 at said server machine.

Claim 14 (canceled)

1 Claim 15 (currently amended): A method for enabling an identity change during a certificate-
2 based host access session, comprising the steps of:

3 processing a first sign-on during a secure session using a digital certificate, further
4 comprising the steps of:

5 establishing said secure session from a client machine to a server machine using
6 said digital certificate, wherein said digital certificate represents an identity of said client machine
7 or a user thereof;

8 storing said digital certificate or a reference thereto at said server machine;

9 establishing a session from said server machine to a host system using a legacy
10 host communication protocol, responsive to receiving, at said server machine, a first sign-on
11 request from said client machine, wherein said first sign-on request identifies a first secure legacy
12 host application to which said first sign-on is requested;

13 passing said stored digital certificate or said reference from said server machine to
14 a host access security system;

Serial No. 09/619,912

-10-

Docket RSW9-2000-0081-US1

15 authenticating, by said host access security system, said identity using said passed
16 digital certificate or a retrieved certificate which is retrieved using said reference;

17 using, by said host access security system, said passed or retrieved digital
18 certificate to locate access credentials for said user;

19 accessing, by said host access security system, a stored password or generating a
20 password substitute representing said located credentials;

21 returning, by said host access security system, said stored password or generated
22 password substitute to said server machine, along with a first user identifier corresponding to said
23 located credentials;

24 requesting by said first secure legacy host application, responsive to said
25 computer-readable program code means for establishing said session, first sign-on information for
26 said user; and

27 responding to said request for first sign-on information by sending a first sign-on
28 message with placeholder syntax from said client machine to said server machine, said placeholder
29 syntax representing a user identification and a password of said user, wherein said user
30 identification and said password are expected in said first sign-on message by said first secure
31 legacy host application; and

32 using, by said server machine, said returned password or password substitute and
33 said returned first user identifier to transparently complete said first sign-on, on behalf of said user
34 of said client machine, to said first secure legacy host application executing at said host system by
35 substituting said returned first user identifier and said returned password or password substitute
36 for said placeholder syntax in said first sign-on message, thereby creating a revised first sign-on

37 message, and forwarding said revised first sign-on message from said server machine to said first
38 secure legacy host application;; and

39 processing a second sign-on during said secure session, without requiring establishment of
40 a new secure session between said client machine and said server machine, using a second digital
41 certificate that represents a second identity, further comprising the steps of:

42 receiving a second sign-on request, at said server machine from said client
43 machine, wherein: (1) said second sign-on request identifies a second secure legacy host
44 application to which said second sign-on is requested; (2) said second sign-on request includes
45 said second digital certificate, or a second certificate reference that references said second digital
46 certificate, for said second identity; (3) said second secure legacy host application may be identical
47 to said first secure legacy host application; and (4) said second identity is for a second user,
48 wherein said second user may be identical to said user;

49 passing said second digital certificate or said second certificate reference from said
50 server machine to said host access security system;

51 authenticating, by said host access security system, said second identity using said
52 passed second digital certificate or a second retrieved certificate which is retrieved using said
53 second certificate reference;

54 using, by said host access security system, said passed second digital certificate or
55 said second retrieved certificate to locate second access credentials for said second user;

56 accessing, by said host access security system, a second stored password or
57 generating a second password substitute representing said second located credentials;

58 returning, by said host access security system, said second stored password or

59 second generated password substitute to said server machine, along with a second identifier
60 corresponding to said second located credentials; and
61 using, by said server machine, said returned second password or second password
62 substitute and said returned second user identifier to transparently complete said second sign-on,
63 on behalf of said second user of said client machine, to said second secure legacy host application
64 executing at said host system.

1 Claim 16 (previously presented): The method as claimed in Claim 15, wherein said digital
2 certificate and said second digital certificate are X.509 certificates and said digital certificate
3 reference and second certificate reference are references to an X.509 certificate.

1 Claim 17 (original): The method as claimed in Claim 15, wherein said communication protocol is
2 a 3270 emulation protocol.

1 Claim 18 (original): The method as claimed in Claim 17, wherein said host access security system
2 is a Resource Access Control Facility (RACF) system.

1 Claim 19 (previously presented): The method as claimed in Claim 15, wherein said step of
2 processing said second sign-on further comprises the step of storing said second digital certificate
3 at said server machine.

Claim 20 (canceled)

Serial No. 09/619,912

-13-

Docket RSW9-2000-0081-US1

1 Claim 21 (currently amended): The computer program product as claimed in Claim 1, wherein:

2 said computer-readable program code means for processing said second sign-on further
3 comprises computer-readable program code means for receiving, at said server machine, a second
4 sign-on message sent from said client machine, wherein said second sign-on message has
5 placeholders placeholder syntax representing a user identification of said second user and a
6 password of said second user, wherein said user identification of said second user and said
7 password of said second user are expected in said second sign-on message by said second secure
8 legacy host application; and

9 said computer-readable program code means for using said returned second password or
10 second password substitute and said returned second user identifier to transparently complete said
11 second sign-on further comprises:

12 computer-readable program code means for substituting said returned second user
13 identifier and said returned second password or second password substitute for said placeholders
14 placeholder syntax in said second sign-on message, thereby creating a revised second sign-on
15 message; and

16 computer-readable program code means for forwarding said revised second sign-
17 on message from said server machine to said second secure legacy host application.

1 Claim 22 (previously presented): The computer program product according to Claim 1, wherein
2 said second sign-on request includes information usable as proof that said second user owns said
3 second digital certificate.

1 Claim 23 (previously presented): The computer program product according to Claim 22, wherein
2 said proof further comprises a random seed value and a sequence number concatenated thereto by
3 said client machine to detect replay attacks, wherein said random seed value was previously sent
4 from said server machine to said client machine.

1 Claim 24 (previously presented): The computer program product according to Claim 23, wherein
2 said identification of said second secure legacy host application is also concatenated to said
3 random seed value.

1 Claim 25 (previously presented): The computer program product according to Claim 23, wherein
2 a digital signature computed using a private key associated with said second digital certificate is
3 included in said second sign-on request, said digital signature covering said random seed value
4 and said concatenated sequence number.

1 Claim 26 (previously presented): The computer program product according to Claim 24, wherein
2 a digital signature computed using a private key associated with said second digital certificate is
3 included in said second sign-on request, said digital signature covering said random seed value,
4 said concatenated sequence number, and said concatenated identification of said second secure
5 legacy host application.

1 Claim 27 (currently amended): The system as claimed in Claim 9, wherein:

Serial No. 09/619,912

-15-

Docket RSW9-2000-0081-US1

2 said means for processing said second sign-on further comprises means for receiving, at
3 said server machine, a second sign-on message sent from said client machine, wherein said second
4 sign-on message has ~~placeholders~~ placeholder syntax representing a user identification of said
5 second user and a password of said second user, wherein said user identification of said second
6 user and said password of said second user are expected in said second sign-on message by said
7 second secure legacy host application; and

8 said means for using said returned second password or second password substitute and
9 said returned second user identifier to transparently complete said second sign-on further
10 comprises:

11 means for substituting said returned second user identifier and said returned
12 second password or second password substitute for said ~~placeholders~~ placeholder syntax in said
13 second sign-on message, thereby creating a revised second sign-on message; and

14 means for forwarding said revised second sign-on message from said server
15 machine to said second secure legacy host application.

1 Claim 28 (currently amended): The method as claimed in Claim 15, wherein:

2 said step of processing said second sign-on further comprises the step of receiving, at said
3 server machine, a second sign-on message sent from said client machine, wherein said second
4 sign-on message has ~~placeholders~~ placeholder syntax representing a user identification of said
5 second user and a password of said second user, wherein said user identification of said second
6 user and said password of said second user are expected in said second sign-on message by said
7 second secure legacy host application; and

8 said step of using said returned second password or second password substitute and said
9 returned second user identifier to transparently complete said second sign-on further comprises
10 the steps of:

11 substituting said returned second user identifier and said returned second password
12 or second password substitute for said ~~placeholders~~ placeholder syntax in said second sign-on
13 message, thereby creating a revised second sign-on message; and

14 forwarding said revised second sign-on message from said server machine to said
15 second secure legacy host application.

1 Claim 29 (currently amended): A computer-implemented method for enabling an identity change
2 during a certificate-based host access session, comprising steps of:

3 establishing a secure session between a client and a server using a digital certificate owned
4 by a user of said client;

5 remembering said digital certificate at said server;

6 completing a first sign-on to a host application, by said server on behalf of said user,
7 responsive to receiving an asynchronous sign-on request from said client that identifies said host
8 application, further comprising the steps of:

9 using said remembered digital certificate to authenticate said user to a host access
10 security component;

11 if said user is authenticated, locating, by said host access security component,
12 access credentials of said user;

13 creating, by said host access security component, a passticket that represents said

14 located access credentials;

15 returning said passticket from said host access security component to said server,

16 along with a user identifier associated with said located access credentials; and

17 inserting, by said server, said passticket and said user identifier into a log-on

18 message in place of placeholders therefor for a user password and said user identifier, when said

19 log-on message is received at said server from said client, thereby creating a revised log-on

20 message, in a form expected by said host application, that is then sent from said server to sign said

21 user on to said host application; and

22 completing a second sign-on to a second host application, by said server on behalf of a

23 second user, responsive to receiving a second asynchronous sign-on request from said client that

24 identifies said second host application, wherein said second host application may be identical to

25 said host application and said second user may be identical to said user, further comprising the

26 steps of:

27 using a new digital certificate and proof therefor to authenticate said second user

28 to said host access security component, wherein said new digital certificate and said proof

29 therefor are included in said second asynchronous sign-on request;

30 if said second user is authenticated, locating, by said host access security

31 component, access credentials of said second user;

32 creating, by said host access security component, a second passticket that

33 represents said located access credentials of said second user;

34 returning said second passticket from said host access security component to said

35 server, along with a second user identifier associated with said located access credentials of said

36 second user; and
37 inserting, by said server, said returned second passticket and said returned second
38 user identifier into a second log-on message in place of placeholders ~~therefor~~ for a second user
39 password and said second user identifier, when said second log-on message is received at said
40 server from said client, thereby creating a revised second log-on message, in said form expected
41 by said second host application, that is then sent from said server to sign said second user on to
42 said second host application.

1 Claim 30 (new): A method of providing identity change during a secure session, comprising steps
2 of:

3 upon receiving a first log-on message containing placeholder syntax from a client during a
4 secure session, substituting therefor a first user identifier and a first password substitute provided
5 by a host access security system upon authentication of user credentials associated with the client
6 and with a user thereof, thereby creating a revised first log-on message in a form expected by a
7 first legacy host application, the first password substitute representing access privileges associated
8 with the user credentials for the first legacy host application;

9 forwarding the revised first log-on message to the first legacy host application for
10 completing a secure sign-on thereto;

11 upon receiving a second log-on message containing placeholder syntax from the client
12 during the secure session, substituting therefor a second user identifier and a second password
13 substitute provided by the host access security system upon authentication of second user
14 credentials associated with the client and with the user thereof or a different user thereof, thereby

15 creating a revised second log-on message in a form expected by a second legacy host application,
16 the second password substitute representing access privileges associated with the second user
17 credentials for the second legacy host application, wherein the second legacy host application may
18 be identical to the first legacy host application; and
19 forwarding the revised second log-on message to the second legacy host application for
20 completing a secure sign-on thereto.